Here's the kind of data hackers get about you from hospitals

September 23 2019

Table 2. Types of Information Compromised in PHI Breaches

Type of Information Compromised	Breaches, *n* (%) (*n* = 1461)	Patients Affected, *n* (%) (*n* = 168 679 321)
Demographic characteristics (e.g., name, address, e-mail address, and other personal identifiers)	1461 (100)	168 679 321 (100)
Sensitive demographic characteristics (Social Security number, driver's license number, or date of birth)*	964 (66)	149 512 186 (89)
Service or financial information (e.g., billing, dates of service, and payment information)	513 (35)	60 236 502 (36)
Sensitive financial information (payment card or bank account)	186 (13)	49 304 299 (29)
Breaches involving sensitive demographic characteristics or financial information†	1042 (71)	158 851 286 (94)
Medical or clinical information (e.g., diagnosis, laboratory results, treatment, and prescriptions)	944 (65)	47 705 243 (28)
Sensitive medical information (substance abuse, HIV, sexually transmitted diseases, mental health, or cancer)	22 (2)	2 422 155 (1)
Medical or clinical information without any overlap with demographic characteristics or financial information	239 (16)	6 255 255 (4)

PHI = protected health information.
* In this group, we include 94 breaches affecting 2 203 108 patients that didn't mention the specifics of demographic characteristics but offered free credit monitoring to victims.
† Given that 1 PHI breach can compromise 1 or several types of PHI, the total number of breaches involving sensitive demographic characteristics or financial information is smaller than the sum of breaches involving sensitive demographic characteristics and breaches involving sensitive financial information.

All 1,461 breaches involved at least one piece of demographic information. Credit: John Jiang, Ge Bai

When hospitals are hacked, the public hears about the number of victims—but not what information the cybercriminals stole. New research from Michigan State University and Johns Hopkins University is the first to uncover the specific data leaked through hospital breaches, sounding alarm bells for nearly 170 million people.

"The major story we heard from victims was how compromised, sensitive information caused financial or reputation loss," said John

(Xuefeng) Jiang, lead author and MSU professor of accounting and information systems. "A criminal might file a fraudulent tax return or apply for a credit card using the social security number and birth dates leaked from a hospital data breach."

Until now, researchers have not been able to classify the kind or amount of public health information leaked through breaches; thus, never getting an accurate picture of breadth or consequences.

The findings, published in *Annals of Internal Medicine*, encompass 1,461 breaches that happened between Oct. 2009 and July 2019.

Jiang and co-author Ge Bai, associate professor of accounting at Johns Hopkins Carey Business School and Bloomberg School of Public Health, discovered that 169 million people have had some form of information exposed because of hackers.

To uncover what specific information was exposed, the researchers classified data into three categories: demographic, such as names, email addresses and other personal identifiers; service or financial information, which included service date, billing amount, payment information; and medical information, such as diagnoses or treatment.

"We further classified social security and driver's license numbers and birth dates as sensitive demographic information, and payment cards and banking accounts as sensitive financial information. Both types can be exploited for identity theft or financial fraud," Jiang said. "Within medical information, we classified information related to substance abuse, HIV, sexually transmitted diseases, mental health and cancer as sensitive medical information because of their substantial implications for privacy."

Over 70% of the breaches compromised sensitive demographic or

financial data that could lead to identity theft or financial fraud. More than 20 breaches compromised sensitive health information, which affected 2 million people.

"Without understanding what the enemy wants, we cannot win the battle," Bai said. "By knowing the specific information hackers are after, we can ramp up efforts to protect patient information."

With a newfound understanding of what explicit data was leaked—and how many over the last decade were affected—the researchers offer hospitals and health providers suggestions on how to better protect patients' sensitive information.

The researchers suggest that the Department of Health and other regulators formally collect the types of information compromised in a data breach to help the public assess the potential damages. Hospitals and other healthcare providers, Jiang said, could effectively reduce data breach risks by focusing on securing information if they have limited resources. For example, implementing separate systems to store and communicate sensitive demographic and financial information.

Jiang noted that the Department of Health and Human Services and Congress recently proposed rules that encourage more data-sharing, which increases the risks for breaches. He said that he and Bai plan to work with lawmakers and industries by providing practical guidance and advice using their academic findings.

More information: *Annals of Internal Medicine* (2019). annals.org/aim/article/doi/10.7326/M19-1759

Provided by Michigan State University